LOCKS LAW FIRM, LLC
By: Michael A. Galpern, Esquire (Attorney No.: 029031988)
Andrew P. Bell, Esquire (Attorney No.: 025052010)
James A. Barry, Esquire (Attorney No.: 027512008)
801 N. Kings Highway
Cherry Hill, NJ 08034
Tel: (856) 663-8200

Attorneys for Plaintiff and the Putative Class

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY
(Newark Vicinage)

ALANA M. BRADLEY on behalf of herself and other persons similarly situated, **Plaintiffs(s)** **v.** **EQUIFAX, INC.** **Defendant(s)**	CIV. ACTION NO.: Civil Action **CLASS-ACTION COMPLAINT AND DEMAND FOR JURY TRIAL**

Plaintiff, Alana M. Bradley, by way of Complaint on behalf of herself and others similarly situated, individually and as class representative, upon information and belief, except for the allegations concerning Plaintiff's own actions, says as follows:

INTRODUCTION

1. This is a class-action Complaint brought by Plaintiff, Alana M. Bradley ("Plaintiff") on her own behalf and on behalf of all others similarly situated against Defendant, Equifax, Inc., to obtain declaratory, injunctive and monetary relief for a class of individuals against Defendant for its failure to safeguard its client's Personally Identifiable Information ("PII") including names, Social Security Numbers, birth dates,

addresses and driver's license numbers, and for failing to provide timely, accurate and adequate notice to Plaintiff and other Class Members that their PII had been stolen and failing to provide timely, accurate and adequate notice of precisely what types of information were stolen for each consumer.

2. On September 7, 2017, Equifax announced a nationwide data breach affecting an estimated 143 million consumers in the United States. According to Equifax, the breach not only disclosed PII for 143 million consumers, it also included credit card numbers for about 209,000 people and dispute documents with PII for approximately 182,000 people.[1] According to Equifax the breach occurred from mid-May through July.[2] Despite the fact that the breach was apparently discovered on or about July 29, 2017, Equifax did not notify consumers of the breach until September 7, 2017.[3]

3. While Equifax delayed in notifying consumers of the data breach high level executives sold shares of company stock. Specifically, Chief Financial Officer John W. Gamble sole nearly $1 million worth of stock on August 1, 2017; President of U.S. Information Solutions, Joseph M. Loughran III, sold approximately $700,000 worth of stock on August 1, 2017 and President of Workforce Solutions, Rodolfo O. Ploder sold approximately $250,000 worth of stock on August 2, 2017.[4]

---

[1] *See* Federal Trade Commission, *The Equifax Data Breach: What to Do*, September 8, 2017. *Available at*: https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do (last accessed September 18, 2017)

[2] *Ibid.*

[3] *See* Sara Ashley O'Brien, *Giant Equifax data breach: 143 million people could be affected*, CNN tech, September 8, 2017. *Available at*: http://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html (last accessed September 18, 2017)

[4] Renae Merle, Outrage builds after Equifax executives banked $2 million in stock sales following data breach, The Washington Post, September 8, 2017. *Available at:* https://www.washingtonpost.com/news/business/wp/2017/09/08/outrage-builds-after-equifax-executives-

4. The data breach occurred because Equifax failed to implement adequate security measures to safeguard consumers' PII and willfully ignored *known* weaknesses in its data security, specifically, Equifax failed to install a security patch in its software which was provided to Equifax on March 7, 2017.[5] Unauthorized parties routinely attempt to gain access to and steal personal information from networks and information systems – especially from entities such as Equifax, which are known o possess a large number of individuals' valuable personal and financial information.

5. Armed with consumers' PII, identity thieves can commit a variety of crimes that harm victims of a data breach. For instance, they can take out loans, mortgage property, open financial accounts, open credit cards in a victim's name, use a victim's information to obtain government benefits or file fraudulent returns to obtain a tax refund, obtain a driver's license or identification card in a victim's name, or give false information to police during an arrest. Hackers also routinely sell individuals' PII to other individuals who intend to misuse the information.

6. As a result of Equifax's willful failure to prevent the breach, Plaintiff and Class Members have been exposed to fraud, identity theft, and financial harm, as detailed below, and to a heightened, imminent risk of such harm in the future. Plaintiff and Class Members have to monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Class Members also have and will continue to incur, additional out-of-pocket costs for obtaining credit reports, credit

---

banked-2-million-in-stock-sales-following-data-breach/?utm_term=.8a85a1f498a2 (last accessed September 18, 2017).

[5] *See* The Apache Software Foundation, MEDIA ALERT: The Apache Software Foundation Confirms Equifax Data Breach Due to Failure to Install Patches Provided for Apache® Struts™ Exploit, September 14, 2017. (Last accessed September 18, 2017)

freezes, credit monitoring services, and other protective measures in order to detect, protect, and repair the data breach's impact on their PII for ht remainder of their lives.

7. As described By Gasan Awad, Vice President, identity and fraud product management for Equifax "Data breaches are the first step for criminals with intentions to steal and misuse consumer information. Once fraudsters have consumers' private identity information they then take the next step in criminal activity, often committing fraud by opening fraudulent accounts or taking over an existing account. In essence, fraudsters use the personal information obtained from the breaches to apply for credit or benefits or hijack existing accounts, all while acting as the victims."[6]

8. Plaintiff brings this action to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiff seeks the following remedies, among others: statutory damages under the Fair Credit Reporting Act ("FCRA") and state consumer protection statutes, reimbursement of out-of-pocket losses, other compensatory damages, credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Equifax to implement improved data security measures.

PARTIES

9. Plaintiff, Alana M. Bradley, is an adult individual residing in Cherry Hill New Jersey who has confirmed that her information was disclosed in the data breach through Defendant's website, www.equifaxsecurity2017.com/potential-impact/. Since the breach was announced Ms. Bradley has received multiple unauthorized charges to her Chase Visa card. As a result of the breach she has enrolled in credit monitoring services

[6] Awad, Gasan *Device Advice: Keeping Fraudsters from Consumer Info*, Dark Reading, April 19, 2016. *Available at:* https://www.darkreading.com/endpoint/device-advice-keeping-fraudsters-from-consumer-info/a/d-id/1325182 (last accessed September 19, 2017).

through LifeLock, at a monthly rate of $9.99 per month. She has also spent time and effort monitoring her financial accounts.

10. Defendant, Equifax, Inc. is a Delaware corporation with its principal place of business located at 1550 Peachtree Street NE Atlanta, Georgia 30309. Equifax regularly transacts business within the District of New Jersey.

JURISDICTION AND VENUE

11. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because Plaintiff is bringing claims under the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681e, *et seq*.

12. This Court also has diversity jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action involving more than 100 Class Members, the amount in controversy exceeds $5 million exclusive of interest and costs, and many members of the Class are citizens of states different from Defendants.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Plaintiff and Members of the Class reside in the District, and Equifax regularly transacts business here.

FACTUAL ALLEGATIONS

14. Equifax is one of the major credit reporting bureaus in the United States. As a credit bureau service, Equifax is engaged in a number of credit-related services, as described by Equifax "[t]he company organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million business worldwide, and its database includes employee data contributed from more than 7,100 employers."[7] As a

[7] *See Equifax Company Profile,* Equifax, http://www.equifax.com/about-equifax/company-profile (last accessed September 18, 2017).

credit bureau service, Equifax maintains information related to the credit history of consumers and provides the information to credit grantors who are considering a borrower's application for credit or who have extended credit to the borrower.

15. As described by Equifax, "[b]usinesses rely on us for consumer and business credit intelligence, credit portfolio management, fraud detection, decisioning technology, marketing tools, and human resources-related services. We also offer products that enable individual consumers to manage their financial affairs and protect their identity."[8]

16. Prior to the Data Breach, Equifax promised its customers and everyone about whom it collects PII that it would reasonably protect their PII. Equifax's privacy policy stated, in relevant part: "We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers."[9]

17. Plaintiff's and Class Members' PII was disclosed to Equifax, and Equifax compiled, maintained, and furnished Class Members' PII, in connection with Class Members' acquisition of services, through Defendant's services as a credit bureau. Equifax is allowed to perform such services, involving such sensitive information, only if it adheres to the requirements of laws meant to protect the privacy of such information, such as the FCRA and the Gramm-Leach-Bliley Act ("GLBA"). Equifax's maintenance, use, and furnishing of such PII is and was intended to affect Plaintiff and other Class Members, and the harm caused by disclosure of that PII in the Data Breach was entirely

[8] *See* 2015 Equifax Annual Report, pg 12. Available at: http://files.shareholder.com/downloads/ABEA-32806R/1877079758x0x882810/CC30F45C-8BF7-4814-8A29-A7CE1D85EDCA/15-1002_2015_Annual_Report_Interactive_PDF_FINAL_032116.pdf (last accessed September 18, 2017).
[9] http://www.equifax.com/privacy/ (last accessed September 18, 2017)

foreseeable to Equifax.

18. Equifax touts itself as an industry leader in data breach security and often promotes the importance of data breach prevention. Equifax offers services directly targeted to assisting businesses who have encountered a data breach.[10]

19. Despite that fact, Defendant failed to update its software to provide basic security for consumers, and failed to timely notify consumers of the data breach, as alleged in paragraphs 2-4 of the present complaint.

20. Since identity thieves use the PII of other people to commit fraud or other crimes, Plaintiff and other consumers whose information was exposed in the Data Breach are subject to an increased, concrete risk of identity theft. Javelin Strategy & Research, a research-based consulting that specializes in fraud and security in advising its clients, reported in its 2014 Identity Fraud Study that "[d]ata breaches are the greatest risk factor for identity fraud." In fact, "[i]n 2013, one in three consumers who received notification of a data breach became a victim of fraud." Javelin also found increased instances of fraud other than credit card fraud, including "compromised lines of credit, internet accounts (*e.g.*, eBay, Amazon) and email payment accounts such as PayPal."[11]

21. The exposure of Plaintiff's and Class Members' Social Security numbers in particular poses serious problems. Criminals frequently use Social Security numbers to create false bank accounts, file fraudulent tax returns, and incur credit in the victim's name. Neal O'Farrell, a security and identity theft expert for Credit Sesame calls a Social Security number "your secret sauce," that is "as good as your DNA to hackers."[12] Even

[10] *See, e.g.* http://www.equifax.com/business/equifax-breach-products (last accessed September 18, 2017).
[11] *See* https://www.javelinstrategy.com/press-release/new-identity-fraud-victim-every-two-seconds-2013-according-latest-javelin-strategy (last visited September 18, 2017).
[12] Tips, How to Protect Your Kids From the Anthem Data Breach," Kiplinger (Feb. 10, 2015), *available at*

where data breach victims obtain a new Social Security number, the Social Security Administration warns "that a new number probably will not solve all [] problems . . . and will not guarantee [] a fresh start."[13] In fact, "[f]or some victims of identity theft, a new number actually creates new problems." One of those new problems is that a new Social Security number will have a completely blank credit history, making it difficult to get credit for a few years unless it is linked to the old compromised number.

22. As a result of the compromising of their personal information, Plaintiff and Class Members will face an increased risk of experiencing the following injuries:

- money and time expended to prevent, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of personal information;
- money and time lost as a result of fraudulent access to and use of their financial accounts;
- loss of use of and access to their financial accounts and/or credit;
- money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;
- impairment of their credit scores, ability to borrow, and/or ability to obtain credit;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;
- costs and lost time obtaining credit reports in order to monitor their credit records;
- costs of credit monitoring, as Defendant has offered none to date;
- costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;
- money and time expended to ameliorate the consequences of the filing of fraudulent tax returns;
- lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach, including but not

---

http://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html (last visited September 18, 2017).

[13] Social Security Administration, Identity Theft and Your Social Security Number, pp. 7-8, *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited September 18, 2017)

limited to efforts to research how to prevent, detect, contest, and recover from misuse of their personal information;

- loss of the opportunity to control how their personal information is used; and
- continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Equifax fails to undertake appropriate, legally required steps to protect the personal information in its possession.

23. The Gramm-Leach-Bliley Act ("GLBA") imposes upon "financial institutions" "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801. To satisfy this obligation, financial institutions must satisfy certain standards relating to administrative, technical, and physical safeguards:

> (1) to ***insure the security and confidentiality of customer records and information***;
>
> (2) to ***protect against any anticipated threats or hazards to the security or integrity of such records***; and
>
> (3) to ***protect against unauthorized access to or use of such records*** or information which could result in substantial harm or inconvenience to any customer. 15 U.S.C. § 6801(b) (emphasis added).

24. In order to satisfy their obligations under the GLBA, financial institutions must "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [their] size and complexity, the nature and scope of [their] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.4. "In order to develop, implement, and maintain [their] information security program, [financial institutions] shall:

(a) Designate an employee or employees to coordinate [their] information security program.

(b) ***Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information*** that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of [their] operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) ***Design and implement information safeguards to control the risks [they] identify through risk assessment***, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring [their] service providers by contract to implement and maintain such safeguards.

(e) ***Evaluate and adjust [their] information security program in light of the results*** of the testing and monitoring required by paragraph (c) of this section; any material changes to [their] operations or business arrangements; or any other circumstances that [they] know or have reason to know may have a material impact on [their] information security program."

Id.

25. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F, financial institutions have an affirmative

duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id.* "At a *minimum*, an institution's response program should contain procedures for the following:

> a. Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused;
>
> b. Notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, as defined below;
>
> c. Consistent with the Agencies' Suspicious Activity Report ("SAR") regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;
>
> d. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and
>
> e. Notifying customers when warranted.

Id. (emphasis added).

26. Further, "[w]hen a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible." *Id.*

27. Credit bureaus are "financial institutions" for purposes of the GLBA,

and are therefore subject to its provisions. *See TranUnion LLC v. F.T.C.*, 295 F.3d 42, 48 (D.C. Cir. 2002). Under Regulation Y promulgated by the Federal Reserve Board, *Bank Holding Companies and Change in Bank Control*, "credit bureau services[14]" are "so closely related to banking or managing or controlling banks as to be a proper incident thereto." Since Equifax is a credit bureau and performs credit bureau services, it qualifies as a financial institution for purposes of the GLBA.

28. "Nonpublic personal information," includes PII (such as the PII compromised during the Data Breach) for purposes of the GLBA. Likewise, "sensitive customer information" includes PII for purposes of the Interagency Guidelines Establishing Information Security Standards.

29. Upon information and belief, Equifax failed to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Equifax's failure to implement and maintain adequate data security practices to safeguard Class Members' PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class Members' PII.

30. Upon information and belief, Equifax also failed to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems" as mandated by the GLBA. This includes, but is not limited to, Equifax's failure to notify appropriate regulatory agencies,

[14] Credit bureau services include ""[m]aintaining information related to the credit history of consumers and providing the information to a credit grantor who is considering a borrower's application for credit or who has extended credit to the borrower." *See* 12 C.F.R. § 225.28.

law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

31. Equifax has also failed to notify affected customers as soon as possible after it became aware of unauthorized access to sensitive customer information, and has failed to communicate directly with Class Members to date.

CLASS ACTION ALLEGATIONS

32. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23(b)(1), (b)(2), (b)(3), and (c)(4).

A. Nationwide Class

33. Plaintiff brings the FCRA, negligence, and negligence per se claims (Counts I-IV) on behalf of a proposed nationwide class ("Nationwide Class"), defined as follows:

> *All natural persons in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017.*

B. New Jersey Subclass

34. Plaintiff also, and in the alternative to claims asserted on behalf of the Nationwide Class, asserts claims under the laws of New Jersey, and on behalf of a separate New Jersey class ("New Jersey Class"), defined as follows:

> *All natural persons in New Jersey whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017.*

35. The Class and Subclass for those whose benefit this action has been brought is so numerous that joinder of all members is impracticable, as Defendant has

indicated it believes as many as 143 million individuals may have been impacted in the Breach.

36. Plaintiff's claims are typical of the claims of the members of the Class, since all such claims arise out of Defendant's failure to safeguard user's information, and Plaintiff has confirmed that her information was disclosed in the data breach.

37. Plaintiff does not have interests antagonistic to the interests of the Class or Subclass.

38. The Class and Subclass, of which Plaintiff is a member, are readily identifiable by reference to Defendant's records.

39. Plaintiff will fairly and adequately protect the interests of the Class and Subclass and have retained competent counsel experienced in the prosecution of consumer litigation. Proposed Class Counsel has investigated and identified potential claims in the action; has a great deal of experience in handling class actions, other complex litigation, and claims of the type asserted in this action.

40. There are common questions of law and fact effecting the rights of all class members, including the following:

a. Whether Equifax violated the FCRA, GLBA, and New Jersey law by failing to implement reasonable security measures;

b. Whether Equifax violated common and statutory law by failing to promptly notify Class Members their Personal Identifying Information had been compromised;

c. Whether class members may obtain injunctive relief against Equifax to require that it safeguard or destroy, rather than retain as it has Personal Identifying Information of Plaintiff and the Class Members;

d. Which security procedures and which data-breach notification procedure Equifax should be required to implement as part of any injunctive relief ordered by the Court;

e. Whether Equifax was negligent in its securing of Plaintiff and Class Members' PII;

f. Whether Equifax has complied with implied contractual obligations to use reasonable security measures;

g. What security measures, if any, must be implemented by Equifax to comply with its implied contractual obligations;

h. Whether Equifax violated New Jersey privacy laws in connection with the actions described here; and

i. What the nature of the relief should be, including equitable relief, to which Plaintiff and Class Members are entitled.

41. A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. While the economic damages suffered by the individual Class Members are significant, the amount is modest compared to the expense and burden of individual litigation. A class action will cause an orderly and expeditious administration of the claims of the Class and will foster economies of time, effort and expense.

42. The questions of law and/or fact common to the members of the Class predominate over any questions affecting only individual members.

43. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications, which would establish incompatible standards of conduct for the Defendant in this action or the prosecution of separate actions by individual members of the Class would create the risk that adjudications with respect to individual members of the Class and Subclass would as a practical matter be dispositive of the interests of the other members not parties to the adjudications or substantially impair or impede their ability to protect their interests. Prosecution as a class action will eliminate the possibility of repetitious litigation.

44. Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the class as a whole.

45. Plaintiffs do not anticipate any difficulty in the management of this litigation.

COUNT ONE
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT ("FCRA")
(As to the Nationwide Class and the New Jersey Class)

46. Plaintiff incorporates by reference all paragraphs above as if fully set forth herein.

47. As individuals, Plaintiff and Class Members are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

48. Under the FCRA, a "consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly

engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." 15 U.S.C. § 1681a(f).

49. Equifax is a consumer reporting agency under the FCRA because it, for monetary fees, regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

50. As a consumer reporting agency, the FCRA requires Equifax to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

51. Under the FCRA, a "consumer report" is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1).

52. The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Class Members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Class Members' eligibility for credit.

53. As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed the Nationwide Class Member's PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

54. Equifax furnished the Nationwide and New Jersey Class Member's consumer reports by disclosing their consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their consumer reports; knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports; and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports.

55. The Federal Trade Commission ("FTC") has pursued enforcement actions against consumer reporting agencies under the FCRA for failing "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the" FCRA, in connection with data breaches.[15]

56. Equifax willfully violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. The willful nature of Equifax's violations is

[15] Statement of Commissioner Brill (Federal Trade Commission 2011), *available at* <https://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819settlementonestatement.pdf> (last visited September 18, 2017).

supported by, among other things, its failure to implement a security patch provided to it in order to secure consumer's information. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

57. Equifax also acted willfully because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix To Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiff and other members of the classes of their rights under the FCRA.

58. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiff as well as members of the Nationwide Class and New Jersey Class' personal information for no permissible purposes under the FCRA.

59. Plaintiff and the Class Members have been damaged by Equifax's willful failure to comply with the FCRA. Therefore, Plaintiff and each of the Nationwide Class Members are entitled to recover "any actual damages sustained by the consumer . .

. or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A)

60. Plaintiff and the Nationwide Class Members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2), (3).

COUNT TWO
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT ("FCRA")
(As to the Nationwide Class and the New Jersey Class)

61. Plaintiff incorporates by reference all paragraphs above as if fully set forth here.

62. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, its failure to even install a security patch in order to maintain the security of its systems. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

63. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiff's and the Nationwide Class Member's PII and consumer reports for no permissible purposes under the FCRA.

64. Plaintiff and the Nationwide Class Members have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiff and each of the Nationwide Class Members are entitled to recover "any actual damages sustained by the

consumer." 15 U.S.C. § 1681o(a)(1).

65. Plaintiff and the Nationwide Class Members are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

COUNT THREE
NEGLIGENCE
(As to the Nationwide Class and the New Jersey Class)

66. Plaintiff incorporates by reference all paragraphs above as if fully set forth here.

67. Equifax owed a duty to Plaintiff and Class Members, arising from the sensitivity of the information and the foreseeability of its data safety shortcomings resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, updating software as necessary, designing, maintaining, monitoring, and testing Equifax's security systems, protocols, and practices to ensure that Class Members' information adequately secured from unauthorized access.

68. Equifax owed a duty to Class Members to implement intrusion detection processes that would detect a data breach in a timely manner.

69. Equifax also had a duty to delete any PII that was no longer needed to serve client needs.

70. Equifax owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Class Member's PII.

71. Equifax also had independent duties under state laws that required Equifax to reasonably safeguard Plaintiff's and Class Members' PII and promptly notify them about the Data Breach.

72. Equifax had a special relationship with Plaintiff and Class Members from being entrusted with their PII, which provided an independent duty of care. Plaintiff's and other Class Members' willingness to entrust Equifax with their PII was predicated on the understanding that Equifax would take adequate security precautions. Moreover, Equifax had the ability to protect its systems and the PII it stored on them from attack.

73. Equifax's role to utilize and purportedly safeguard Plaintiff's and Class Members' PII presents unique circumstances requiring a reallocation of risk.

74. Equifax breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Class Member's PII; (b) failing to detect the Data Breach in a timely manner; (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class Member's PII; and (d) failing to provided adequate and timely notice of the breach.

75. But for Equifax's breach of its duties, Class Member's PII would not have been accessed by unauthorized individuals.

76. Plaintiff and Class Members were foreseeable victims of Equifax's inadequate data security practices. Equifax knew or should have known that a breach of its data security systems would cause damages to Class Members.

77. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiff's and the Nationwide Class Member's PII and consumer reports for no permissible purposes under the FCRA.

78. As a result of Equifax's willful failure to prevent the Data Breach, Plaintiff and Class Members suffered injury, which includes but is not limited to

exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class Member's PII has also diminished the value of the PII.

79. The damages to Plaintiff and the Class Members were a proximate, reasonably foreseeable result of Equifax's breaches of its duties.

80. Therefore, Plaintiff and Class Members are entitled to damages in an amount to be proven at trial.

COUNT FOUR
NEGLIGENCE PER SE
(As to the Nationwide Class and the New Jersey Class)

81. Plaintiff incorporates by reference all paragraphs above as if fully set forth here.

82. Under the FCRA, 15 U.S.C. §§ 1681e, Equifax is required to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

83. Defendants failed to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA.

84. Plaintiff and Class Members were foreseeable victims of Equifax's violation of the FCRA. Equifax knew or should have known that a breach of its data

security systems would cause damages to Class Members.

85. As alleged above, Equifax was required under the Gramm-Leach-Bliley Act ("GLBA") to satisfy certain standards relating to administrative, technical, and physical safeguards:

> **(1)** to ***insure the security and confidentiality of customer records and information***;
> **(2)** to ***protect against any anticipated threats or hazards to the security or integrity of such records***; and
> **(3)** to ***protect against unauthorized access to or use of such records*** or information which could result in substantial harm or inconvenience to any customer.

86. In order to satisfy their obligations under the GLBA, Equifax was also required to "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.4

87. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id.*

88. Further, when Equifax became aware of " unauthorized access to sensitive customer information," it should have "conduct[ed] a reasonable investigation to promptly determine the likelihood that the information has been or will be misused" and "notif[ied] the affected customer[s] as soon as possible." *See id.*

89. Equifax violated by GLBA by failing to "develop, implement, and

maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Equifax's failure to implement and maintain adequate data security practices to safeguard Class Member's PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class Members' PII.

90. Equifax also violated the GLBA by failing to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." This includes, but is not limited to, Equifax's failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

91. Equifax also violated by the GLBA by failing to notify affected customers as soon as possible after it became aware of unauthorized access to sensitive customer information.

92. Plaintiff and Class Members were foreseeable victims of Equifax's violation of the GLBA. Equifax knew or should have known that its failure to take reasonable measures to prevent a breach of its data security systems, and failure to timely and adequately notify the appropriate regulatory authorities, law enforcement, and Class Members themselves would cause damages to Class Members.

93. Defendants' failure to comply with the applicable laws and regulations, including the FCRA and the GLBA, constitutes negligence *per se*.

94. But for Equifax's violation of the applicable laws and regulations, Class

Members' PII would not have been accessed by unauthorized individuals.

95. As a result of Equifax's failure to comply with applicable laws and regulations, Plaintiff and Class Members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff and Class Members' PII has also diminished the value of the PII.

96. The damages to Plaintiff and the Class Members were a proximate, reasonably foreseeable result of Equifax's breaches of it's the applicable laws and regulations.

97. Therefore, Plaintiff and Class Members are entitled to damages in an amount to be proven at trial.

COUNT FIVE
INVASION OF PRIVACY
(As to the Nationwide Class and the New Jersey Class)

98. Plaintiff incorporates by reference all paragraphs above as if fully set forth here.

99. Defendant, by and through its failure to adequately safeguard Plaintiff and Class Member's PII has made Plaintiff and Class Member's information public.

100. Plaintiff and Class Member's PII was private.

101. The intrusion upon seclusion, suffered by Plaintiff and Class Members would be highly offensive to a reasonable person.

102. Plaintiff and other Class Member's PII is not of legitimate public concern, and there is no legitimate public interest in the public being apprised of said information.

103. Plaintiff and other Class Members did not consent to the disclosure of their PII.

104. As a direct and proximate result of Equifax's conduct Plaintiff and Class Members, Plaintiff and Class Members sustained actual losses and damages as described in detail above. Additionally Plaintiff and Class members are entitled to presumed damages as a result of Defendant's actions.

COUNT SIX
Violation of the NJ Consumer Fraud Act, *N.J.S.A.* 56:8-1, *et seq.*
(As to the New Jersey Class)

105. Plaintiff incorporates by reference all paragraphs above as if fully set forth here.

106. Plaintiffs and the Class bring these claims against Defendant under the New Jersey Consumer Fraud Act.

107. Defendant sells "merchandise" as defined by the New Jersey Consumer Fraud Act by offering credit-related services to consumers.

108. Defendant engaged in unconscionable and deceptive acts and practices, misrepresentation and the concealment, suppression and omission of material facts with respect to the sale and advertisement of their services in violation of *N.J.S.A.* 56:8-2, including by not limited to the following:

a. Misrepresenting material facts, pertaining to their services to consumers by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and Class Members' PII from unauthorized disclosure, release, data breaches and theft;

b. Misrepresenting material facts by representing to Plaintiff and Class Members that they did and would continue to comply with the relevant industry data security standards, state law and federal law with regard to the protection of Plaintiff and Class Members' PII;

c. Defendant knowingly omitted, suppressed and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and the Class Members' PII with the intent that Plaintiff and the Class Members would rely on the omission, suppression and concealment;

d. Defendant engaged in unconscionable and deceptive acts and practices by failing to disclose the Data Breach to Plaintiff and Class Members in a timely and accurate manner in violation of *N.J.S.A.* 56:8-163(a).

109. As a direct and proximate result of Defendant's unconscionable or deceptive acts and practices, Plaintiff and Class Members suffered an ascertainable loss in moneys or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their PII.

110. Plaintiff and Class members are therefore entitled to injunctive relief, equitable relief, actual damages, treble damages, and attorneys' fees and costs pursuant to *N.J.S.A.* 56:8-19.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class Members proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against Equifax as follows:

a. For an Order certifying the Classes as defined here, and appointing Plaintiff and her Counsel to represent the Class;

b. For equitable relief enjoining Equifax from engaging in the wrongful conduct complained of here pertaining to the misuse and/or disclosure of Plaintiff and Class Members' Personal Identifying Information, and from refusing to issue prompt, complete, and accurate disclosures to the Plaintiff and Class Members;

c. For equitable relief compelling Equifax to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class Members the type of Personal Identifying Information compromised.

d. For statutory damages under the FCRA;

e. For an award of actual damages and compensatory damages, in an amount to be determined;

f. For an award of treble damages, as allowable by law;

g. For an award of costs of suit and attorneys' fees, as allowable by law; and

h. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

LOCKS LAW FIRM, LLC

s/Michael A. Galpern
Michael A. Galpern, Esq.
Andrew P. Bell, Esq.
James A. Barry, Esq.
801 N. Kings Highway
Cherry Hill, NJ 08034
Tel: (856) 663-8200
Fax: (856) 661-8400

CERTIFICATION PURSUANT TO *N.J.S.A.* 56:8-1 et. seq.

1. I hereby certify that to my knowledge the matter in controversy is not the subject of any other action pending in any court or of a pending arbitration.

2. To my knowledge, no other action or arbitration procedure is contemplated.

3. I have no knowledge at this time of the names of any other parties who should be joined in this action.

4. I have forwarded a copy of this Complaint to the Attorney General of the State of New Jersey and Camden County Office of Consumer Affairs pursuant to *N.J.S.A.* 56:8-1, *et seq.*

LOCKS LAW FIRM, LLC

s/Michael A. Galpern
Michael A. Galpern, Esq.
Andrew P. Bell, Esq.
James A. Barry, Esq.
801 N. Kings Highway
Cherry Hill, NJ 08034
Tel: (856) 663-8200
Fax: (856) 661-8400

Dated: September 19, 2017